Listing of Claims

1-19. (Cancelled)

20. (New) A method for communicating between a first private computer network and a second private computer network via a public network, the method comprising:

in the first private network having a plurality of devices, a secure access appliance associated with the plurality of devices, and a firewall between the devices and the public network, the secure access appliance receiving status information from the plurality of devices;

the secure access appliance sending a periodic outgoing message including at least one message with information relating to the status of at least one of the devices, wherein the periodic outgoing message is directed to the second private network through the firewall and via the public network;

receiving through the firewall a request message from the second private network responsive to one of the periodic outgoing messages, the request message requesting that the secure access appliance open a tunnel through the firewall, wherein the firewall allows the request message in response to one of the periodic outgoing messages but otherwise restricts the second private network from accessing the first private network without a tunnel;

the secure access appliance opening a tunnel through the firewall in response to the request message to allow access; and

one or more of the plurality of devices in the first private network receiving instruction messages from the second private network, the instructions being received through the tunnel;

wherein the instruction messages are received for a limited period of time and are received to actively manage the one or more devices.

21. (New) The method of claim 20, wherein the appliance maintains information indicating which devices the second network is allowed to interact with through a tunnel, and wherein the second network is not allowed to interact through a tunnel with some devices.

22. (New) The method of claim 20, wherein the first network receives instruction messages for one device, and wherein the appliance has a filter for limiting access to one and only one device.

23. (New) The method of claim 20, wherein the first network receives instruction messages for a plurality of devices, and wherein the appliance has a filter for limiting access to a plurality of specified devices.

24. (New) The method of claim 20, wherein the appliance includes a virtual private network client.

25. (New) The method of claim 20, further comprising logging information related to tunnel openings.

26. (New) The method of claim 20, further comprising continuing to send periodic messages while a tunnel is open.

27. (New) The method of claim 20, further comprising, after a tunnel is closed, including information about the tunnel closing in a subsequent one of the periodic messages.

28. (New) The method of claim 20, wherein the devices include computers.

29. (New) The method of claim 20, wherein the public network is the Internet, the periodic outgoing messages and request message being sent and received via HTTP.

30. (New) A method for a private director network to interact with one or more devices on a first private network via a public network, wherein the networks have firewalls and limited mutual trust, the method comprising:

the director network receiving periodic messages from the first private network via the public network, the periodic messages including status information about a device on the first private network;

the director network sending a request message to the first private network in response to one of the periodic messages, the request message requesting that the first private network open a tunnel through a firewall in the first private network, the request message including information for indicating to a firewall at the first private network that the request message is in response to one of the periodic messages so that the firewall will not block the request message; and

after a tunnel is opened, the director network sending information through the tunnel to actively control the device by exchanging application data with the device, the information being sent during a limited period of time after which the tunnel closes.

31. (New) The method of claim 30, wherein the director network also interacts with one or more devices on a second private network.

32. (New) The method of claim 30, wherein the director network sends information through the tunnel to actively control a plurality of devices on the first private network.

33. (New) The method of claim 32, further comprising maintaining in memory in the director network status information about the devices on the first private network.

34. (New) The method of claim 30, wherein a device on the first private network includes sending information from a workstation, the director network authenticating the user prior to sending information through the tunnel to actively control the device.

35. (New) The method of claim 30, wherein the director network sends information through a secure appliance that includes a virtual private network client.

36. (New) The method of claim 30, wherein the public network is the Internet, the periodic messages and request messages being sent and received via HTTP.

37. (New) A system for securely communicating between a first private network and a second private network through a public network to enable the second private network to interact with one or more devices on the first private network, the first network including a firewall and having at least one device, the system comprising:

a secure access appliance in the first private network for sending an outgoing message through the firewall to the second network via the public network, wherein the outgoing message is a status message sent periodically from the first private network through the firewall to the public network, the outgoing message at least in some instances including status information relating to the device;

the secure access appliance including a tunnel client for opening a tunnel in the firewall responsive to a request message from the second network requesting that the secure access appliance open a tunnel through the firewall, the request message being received from the firewall and not through a persistent virtual private network with the second private network;

the secure access appliance having interfaces to cause communications received from the second private network to be provided to the device for providing active control of the device for a limited period of time.

38. (New) The system of claim 37, wherein the appliance maintains information indicating which devices the second network is allowed to access with a tunnel, and wherein the second network is not allowed to access at least some devices on the first private network.

39. (New) The system of claim 37, wherein the first private network is operatively coupled to multiple devices and receives instruction messages for a plurality of devices.

40. (New) The system of claim 37, wherein the appliance includes a virtual private network client.

41. (New) The system of claim 37, further comprising memory for storing logging information related to tunnel openings.

42. (New) The system of claim 37, wherein the appliance has a filter allowing the second private network to access one and only one device.

43. (New) The system of claim 37, wherein the outgoing messages and request messages are sent and received via HTTP.

44. (New) A system including a network for securely interacting with a device on a remote and non-trusting private network, the system communicating with the private network and the device through a firewall and via a public network, the system comprising:

a controller including a heartbeat monitor application for receiving periodic messages from the private network via the public network, the periodic messages including messages with status information about the device;

the controller for sending a message via the public network to the private network requesting that the private network open a tunnel, and in response to the private network opening a tunnel, for providing information data to actively maintain and monitor the device, the information data being sent during a defined period of time and without using a persistent virtual private network.

45. (New) The system of claim 44, wherein the system includes memory for maintaining status information about one or more devices on the first private network.

46. (New) The system of claim 44, wherein the memory includes status information about devices on other private networks.

47. (New) The system of claim 44, further comprising an appliance operatively coupled to the controller and including a virtual private network client.